REMARKS

Applicants respectfully request reconsideration of the present case in view of the above amendments and the following remarks.

Claims 4-12, 16-26, 28, 30-58, 60, 62-64, 66-67, and 69-81 have been canceled. Claims 1, 3, 13-15, 27, 29, 59, 61, 65, and 68 are now pending. Claims 1, 13, 15, 59, 61, 65, and 68 have been amended. No new matter has been inserted.

Support for the amendments to claims 1 and 59 can be found at least in claims 8 and 12, and in the specification at page 19, line 31 to page 20, line 2, and at page 20, lines 9-10. Amendments to claims 13, 15, 61, 65, and 68 were simply to clarify dependency.

35 U.S.C. § 101

In the Office Action of February 4, 2009, claims 30-39, 46-49, and 56-68 are non-statutory. Applicants respectfully traverse this rejection.

While not conceding the correctness of this rejection, in the interest of advancing prosecution the Applicants have canceled claims 30-39, 46-49, and 56-68 thereby obviating this rejection. Applicants respectfully request that this rejection be withdrawn.

35 U.S.C. § 103(a) – Thompson in view of Griffiths

In the Office Action of February 4, 2009, claims 1, 3-10, 17-20, 27-30, 32-39, 46-49, 56-61, 68-70, and 77-78 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Thompson (U.S. Patent No. 7,027,872) in view of Griffiths (U.S. Patent No. 7,136,999). Applicants respectfully traverse this rejection.

As amended, claim 1 requires "a key generator configured to dynamically generate a crypto key for each data exchange session with an implantable medical device". Claim 1 also requires an external device "configured to establish an inductive telemetric link to the implantable medical device and to download the crypto key to the implantable medical device through the inductive telemetric link". Claim 1 further requires that "the external device configured to then transact the data exchange session with the implantable medical device through a long range telemetric link authenticated with the crypto key."

Thompson discloses "an encryption apparatus" in which data can "be transferred based on a differentiated encryption system". See abstract of Thompson. However, as is made clear by FIG. 4 of Thompson, the implantable medical device 132 itself does not include an encryption engine or decryption engine. There is no suggestion in Thompson that the implantable medical device 132 itself includes a crypto key or would need a crypto key. There is also no suggestion that a crypto key is downloaded to an implantable medical device from an external device.

As such, Thompson fails to teach or suggest that the external device be "configured to establish an inductive telemetric link to the implantable medical device and to download the crypto key to the implantable medical device through the inductive telemetric link" as required by claim 1. Thompson also fails to teach or suggest a key generator "configured to dynamically generate a crypto key for each data exchange session with an implantable medical device" as required by claim 1.

Griffiths fails to cure the deficiencies of Thompson. Griffiths discloses a system wherein

> "Electronic devices are authenticated to each other initially over a short-range wireless link. In particular, a user first enters a given authentication information in each device. Later, when the devices are out-of-range of the wireless link, they may be authenticated to each other without subsequent input." See abstract (emphasis added).

Thus, in the system of Griffiths the user must separately enter authentication information in each device before they are authenticated to each other through, in the preferred embodiment, a radiofrequency link such as Bluetooth.

In sharp contrast, claim 1 requires that the external device be "configured to establish an inductive telemetric link to the implantable medical device and to download the crypto key to the implantable medical device through the inductive telemetric link". Inductive telemetric links are substantially different than other types of wireless telemetric links in that the distance over which the link can take place is extremely small. For example, as clearly stated in the present specification, inductive telemetry typically has a range of about six centimeters. Griffiths discloses nothing about inductive telemetric links. In fact, Griffiths teach away from the use of inductive telemetric links because if Griffiths were to use an inductive telemetric link there

would be no need to separately enter authentication information into each device before they initially authenticate to one another. Rather, the extremely short range (centimeters) of an inductive telemetric link would suffice to ensure that only the proper two devices were in fact communicating with one another.

Griffiths also fails to teach or suggest a key generator "configured to dynamically generate a crypto key for each data exchange session with an implantable medical device" as required by claim 1.

Further, combining Thompson with Griffiths would not result in the present invention as claimed, but rather would result in a system that is unworkable in the context of implantable medical devices. As stated above, the system of Griffiths requires that the user must separately enter authentication in each device before they are authenticated to each other. In the context of an implantable medical device and an external programmer with a dynamically generated crypto key, that scheme would be unworkable because there would be no practical way for a user to separately enter authentication information into each device (e.g., the implantable medical device in the patient and the external programmer) before they were communicating to each other.

For at least these reasons, Applicants assert that the invention of claim 1 is not rendered obvious by the combination of Thompson in view of Griffiths. As claims 3, 13-15, 27, 29, 61, 65, and 68 are dependent on claim 1, they are also not taught or suggested by the combination of Thompson and Griffiths.

For the reasons above, Applicants assert that the combination of Thompson and Griffiths similarly fails to teach or suggest "means for dynamically generating a crypto key uniquely associated with an implantable medical device to authenticate data during a particular data exchange session", "means for establishing a secure connection through an inductive telemetric interface from an external device with an implantable medical device", and "means for downloading the crypto key from the external device to the implantable medical device via the inductive telemetric interface" as required by claim 59. For at least these reasons, Applicants respectfully request that this rejection be withdrawn.

35 U.S.C. § 103(a) – Thompson in view of Griffiths in further view of Lee

In the Office Action of February 4, 2009, claims 79-81 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Thompson in view of Griffiths in further view of Lee (U.S. Patent No. 6,442,432). Applicants respectfully traverse this rejection.

While not conceding the correctness of the rejection, in the interest of advancing prosecution Applicants have canceled claims 79-81. As such, Applicants respectfully request that this rejection be withdrawn.

35 U.S.C. § 103(a) – Thompson in view of Griffiths in further view of Eckmiller

In the Office Action of February 4, 2009, claims 11-16, 40-45, 62-63, 65-67, 71-72, and 74-76 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Thompson in view of Griffiths in further view of Eckmiller (U.S. Patent No. 6,493,587). Applicants respectfully traverse this rejection.

As described above, the combination of Thompson in view of Griffiths fails to teach or suggest the invention of claim 1. Specifically, Thompson in view of Griffiths fails to teach or suggest that the external device be "configured to establish an inductive telemetric link to the implantable medical device and to download the crypto key to the implantable medical device through the inductive telemetric link". Thompson in view of Griffiths also fails to teach or suggest a key generator "configured to dynamically generate a crypto key for each data exchange session with an implantable medical device" as required by claim 1.

Eckmiller fails to cure the deficiencies of Thompson in view of Griffiths. Eckmiller discloses "a system for the protection of neuroprosthesis operation against unauthorized access". See Abstract. In the system of Eckmiller:

> "During production of the components, they are each equipped with a public and a private initial key and also with the public initial keys of the other components. Each component automatically replaces its own set of keys at random time intervals in the order of magnitude of a few seconds. Each component passes the public key to the other components in encrypted form as soon as it has been changed." See col. 9, lines 33-38 (emphasis added).

Thus, the system of Eckmiller depends on initially supplying each component with keys at the time of manufacture. Later distributions of keys are then encrypted with a previous key. Eckmiller provides that "the operation of the neuroprosthesis or the authorized access to internally or externally stored data is only possible if an authorization signal arriving at the internal components from the external component is legitimized by a method which is based solely on features of the internal components and cannot be analyzed, altered or circumvented by any external component." See col. 3, lines 47-53 (emphasis added).

However, Eckmiller fails to teach or suggest an external device configured to "download the crypto key to the implantable medical device through the inductive telemetric link" as required by claim 1. Further Eckmiller fails to teach or suggest a key generator "configured to dynamically generate a crypto key for each data exchange session with an implantable medical device" as required by claim 1. Therefore, the combination of Thompson in view of Griffiths in further view of Eckmiller fails to teach or suggest the invention of claim 1. As claims 13-15 and 65 are dependent on claim 1, they are also not taught or suggested. As such, Applicants respectfully request that this rejection be withdrawn.

35 U.S.C. § 103(a) – Thompson in view of Griffiths in further view of Wheeler et al.

In the Office Action of February 4, 2009, claims 21-25, 50-55, 64, and 73 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Thompson in view of Griffiths in further view of Wheeler et al. (U.S. Publication No. 2002/0016913). Applicants respectfully traverse this rejection.

While not conceding the correctness of the rejection, in the interest of advancing prosecution Applicants have canceled claims 21-25, 50-55, 64, and 73. As such, Applicants respectfully request that this rejection be withdrawn. As such, Applicants respectfully request that this rejection be withdrawn.

Summary

In view of the above amendments and remarks, Applicants assert that the pending claims are in condition for allowance and respectfully requests notification to that effect. If the

Examiner believes a telephone conference would advance the prosecution of this application, the Examiner is invited to telephone the undersigned at the below-listed telephone number.

Respectfully submitted,

August 4, 2009
Date

/Mark E. Deffner/
Mark E. Deffner
Reg. No. 55,103
612-746-4782
Customer Number: 62058